520.43249X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): KIYOTO, et al

Serial No.:

Filed: October 30, 2003

Title: PEER-TO-PEER COMMUNICATION APPARATUS AND COMMUNICATION METHOD

Group:

LETTER CLAIMING RIGHT OF PRIORITY

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

October 30, 2003

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2003-064328 filed March 11, 2003.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/nac
Attachment
(703) 312-6600

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ３月１１日

出 願 番 号
Application Number: 特願２００３－０６４３２８

[ST. 10/C]: [ＪＰ２００３－０６４３２８]

出 願 人
Applicant(s): 株式会社日立製作所

２００３年 ９月２９日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０７９７１４

【書類名】　特許願

【整理番号】　K02016021A

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/28

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ネットワークソリューション事業部内

【氏名】　清藤　聡史

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ネットワークソリューション事業部内

【氏名】　星野　和義

【発明者】

【住所又は居所】　東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

【氏名】　湯本　一磨

【発明者】

【住所又は居所】　東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

【氏名】　日高　稔

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ピアツーピア通信装置および通信方法

【特許請求の範囲】

【請求項１】

ＩＰネットワークに接続され、１対１の対等型通信を行うピアツーピア通信装置であって、

前記ＩＰネットワークに接続された他の通信装置が属するネットワークに関する情報と、前記他の通信装置の利用者に関する情報とを含む第１の制御情報を取得する手段と、

前記ＩＰネットワークに接続された他の通信装置の通信パケットの送受信における暗号規則と認証規則とを含む第２の制御情報を取得する手段と、

を備え、

前記第１の制御情報と前記第２の制御情報とから、前記他の通信装置に送信するＩＰパケットのセキュリティポリシを決定し、前記決定したセキュリティポリシを用いて前記他の通信装置にＩＰパケットを送信する

ことを特徴とするピアツーピア通信装置。

【請求項２】

請求項１に記載のピアツーピア通信装置であって、

前記取得した第１の制御情報を記憶する手段と、

前記取得した第２の制御情報を記憶する手段と、

をさらに備えたことを特徴とするピアツーピア通信装置。

【請求項３】

請求項１もしくは２に記載のピアツーピア通信装置であって、

前記決定した、送信ＩＰパケットに関する第２の制御情報を、前記他の通信装置に通知する手段をさらに備えたことを特徴とするピアーツーピア通信装置。

【請求項４】

請求項１乃至３に記載のピアツーピア通信装置であって、

前記取得した第１の制御情報と前記取得した第２の制御情報とを表示し、前記新たに決定したセキュリティポリシを入力する外部インタフェース手段をさらに

備えたことを特徴とするピアーツーピア通信装置。

【請求項５】

ＩＰネットワークに接続され、ＩＰパケットを用いて１対１の対等型通信を行うピアツーピア通信装置であって、

前記ＩＰパケットの終端および生成を行うＩＰ機能部と、

前記ＩＰパケットに対する認証および暗号化を処理するＩＰｓｅｃ機能部と、

通信装置間におけるピアツーピア通信の確立および切断を処理するピアツーピア通信機能部と、

前記ＩＰネットワークに接続された他の通信装置が属するネットワークおよび前記他の通信装置の利用者に関するプレゼンス情報を格納するプレゼンス情報記憶部と、

前記プレゼンス情報記憶部へのアクセスを制御するプレゼンス情報処理部と、

前記ＩＰネットワークに接続された他の通信装置の通信パケットの送受信における一連の暗号および認証規則を示すセキュリティポリシ情報を格納するセキュリティポリシ情報記憶部と、

前記セキュリティポリシ情報記憶部へのアクセスを制御するセキュリティポリシ処理部と、

使用者からのセキュリティポリシおよびプレゼンス情報の取得要求を行う第１のインタフェース部と、

使用者の、前記セキュリティポリシ情報記憶部へのアクセスを行う第２のインタフェース部と、

使用者の、前記プレゼンス情報記憶部へのアクセスを行う第３のインタフェース部と、

を備え、

前記プレゼンス情報と前記セキュリティポリシ情報とから、前記他の通信装置に送信するＩＰパケットのセキュリティポリシを決定し、前記決定したセキュリティポリシを用いて前記他の通信装置にＩＰパケットを送信する

ことを特徴とするピアツーピア通信装置。

【請求項６】

ＩＰネットワークにおける１対１の対等型通信を行う通信方法であって、

前記ＩＰネットワークに接続された他の通信装置が属するネットワークに関する情報と、前記他の通信装置の利用者に関する情報とを含む第１の制御情報を取得し、

前記ＩＰネットワークに接続された他の通信装置の通信パケットの送受信における暗号規則と認証規則とを含む第２の制御情報を取得し、

前記第１の制御情報と前記第２の制御情報とから、前記他の通信装置に送信するＩＰパケットのセキュリティポリシを決定し、

前記決定したセキュリティポリシを用いて前記他の通信装置にＩＰパケットを送信する

ことを特徴とする通信方法。

【請求項７】

請求項６に記載の通信方法であって、

前記決定した、送信ＩＰパケットのセキュリティポリシ情報を、前記他の通信装置に通知する段階をさらに備えたことを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、1対1の対等型ピアツーピア通信装置に関し、特に、通信相手や通信相手のネットワーク状況に応じた最適な通信セキュリティ規則を適用するピアツーピア通信装置に関する。

【０００２】

【従来の技術】

インターネット電話を代表とするピアツーピア通信において、第三者によって通信内容を盗聴または改竄されることを防ぐために、通信パケットの暗号化や認証が行われる。通信パケットの暗号化や認証は、個々の通信パケットに対してどのような暗号化や認証を行うかといった一連の規則であるセキュリティポリシに従って行われる。なお、このようなセキュリティポリシを格納するデータベースをセキュリティポリシデータベースといい、通常、別途設置されたポリシーサー

バと呼ばれる装置に格納されている。

【０００３】

インターネット技術の標準化組織であるＩＥＴＦでは、インターネットにおけるＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットレベルでのセキュリティ（第三者による通信内容の盗聴や改竄等の防止）を確保するプロトコルとしてＩＰｓｅｃ（ＩＰ　ｓｅｃｕｒｉｔｙ）を策定している（非特許文献１参照）。

【０００４】

これによれば、送信元および送信先のＩＰアドレスとポート番号、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）やＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）といった上位層プロトコルの種別、受信パケットか送信パケットかを示す通信の方向といった情報を用いて、当該ピアツーピア通信に適用すべきセキュリティポリシを選択する。

【０００５】

そして、選択したセキュリティポリシに記述されているセキュリティ要件（パケットを破棄するかしないか、暗号化を行うか認証を行うか、必ず行うか可能な場合のみ行うか等）が適用される。すなわち、送信側の装置は、送信するパケットの送信元アドレスや送信先アドレスから、セキュリティポリシデータベースを検索し、該当するセキュリティポリシにて示されるセキュリティ要件を満たす暗号化や認証処理を行った後、通信相手にパケットを送信する。

【０００６】

同様に、受信側の装置は、受信したパケットの送信元アドレスや送信先アドレスから、セキュリティポリシデータベースを検索し、受信パケットが該当するセキュリティポリシにて示されるセキュリティ要件を満たす暗号化や認証処理が行われているかを検査し、セキュリティ要件を満たしていないパケットは上位層に渡すことなく廃棄する。

【０００７】

インターネットを用いて、２つの通信ノード間で仮想的な専用線を確立するＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）において、ＩＰｓｅ

ｃを用いて通信のセキュリティを確保する技術としては、例えば、非特許文献２に開示されているものがある。

【０００８】

【非特許文献１】

ＩＥＴＦ　ＲＦＣ　２４０１、１９９８年１１月２５日、ｐ．１４－１７

【非特許文献２】

石井貴之、他１名、「透過的で動的なＶＰＮメカニズムを実現」、季刊ＩＰｖ６マガジン、株式会社インプレス、平成１４年８月１８日、Ｓｕｍｍｅｒ　２００２　ＮＯ．２、ｐ．７４－７５

【０００９】

【発明が解決しようとする課題】

上記非特許文献１に記載のＩＰｓｅｃを適用したピアツーピア通信では、送信側装置に登録されているセキュリティポリシのセキュリティ要件が、受信側装置に登録されている要件を満たさない場合、送信側装置が送信したパケットは受信側装置にて受信後廃棄される。従って、相手装置と適切に通信を行うためには、予め通信装置間において互いのセキュリティポリシを交渉または交換し、通信相手装置のセキュリティ要件を満たすセキュリティポリシに基づいて通信を行う必要がある。

【００１０】

また、モバイル端末装置によるピアツーピア通信のように、通信相手装置が同一の場合であったとしても、それが社内ネットワークに接続されている場合には相応のセキュリティが確保済みと考えられるため、セキュリティレベルを落としたセキュリティポリシを用いて暗号処理等を必要としないより軽快な通信を行い、通信相手端末が社外ネットワークに接続されている場合には、よりセキュリティレベルの高いセキュリティポリシを用いた通信が望まれる。

【００１１】

さらに、通信相手が家族や友人・知人かそうでないか、通信内容がビジネスかプライベートか、また単なる宣伝・広告か等により、適切なセキュリティレベルによる通信が期待できる。

【００１２】

しかしながら、通信相手が上述のような各種状況に応じて適切なセキュリティポリシを作成し設定しているとは限らない。例えば、社内ネットワークに接続されたモバイル端末装置が移動し、接続先が社外ネットワークに切り替えられた際、セキュリティポリシが従前の社内ネットワークに適した比較的緩いセキュリティ要件のままであった場合、第３者等によって通信パケットを盗聴や改竄される危険性が高くなる。

【００１３】

一方、非特許文献２に記載の技術では、ネットワーク上に設けた外部のＩＰｓｅｃ通信管理サーバを介して、通信装置相互間でセキュリティポリシ情報の送受信、およびネゴシエーションを行っている。

【００１４】

しかしながら、外部に設置したサーバを用いているため、サーバにてネットワーク上の通信セキュリティポリシを集中的に管理し，通信装置がセキュリティポリシの変更を行えないという問題があり、利用者が通信状況に応じてセキュリティポリシを自由に設定するといった柔軟的な機能を提供することは不可能であった。

【００１５】

本発明では、通信パケットに対する暗号および認証規則を示す情報であるセキュリティポリシと、通信端末の接続ネットワークの情報や通信相手の情報および通信内容の情報といった通信端末の状態を示す情報であるプレゼンス情報とを、通信装置間で互いに交換し、通信状況に応じた適切なセキュリティポリシによって、通信の安全性が確保されたピアツーピア通信を可能とする通信装置を提供することを課題とする。

【００１６】

さらに、利用者が通信状況に応じてセキュリティポリシを自由に設定することを可能とする通信装置を提供することを課題とする。

【００１７】

【課題を解決するための手段】

上記課題を解決するために本発明では、ＩＰネットワークに接続された他の通信装置が属するネットワークおよび前記他の通信装置の利用者に関するプレゼンス情報を取得する手段と、前記他の通信装置の通信パケットの送受信における一連の暗号および認証規則を示すセキュリティポリシ情報を取得する手段とを備え、前記プレゼンス情報と前記セキュリティポリシ情報とから、前記他の通信装置に送信するＩＰパケットのセキュリティポリシを決定し、前記決定したセキュリティポリシを用いて前記他の通信装置にＩＰパケットを送信するようにした。

【００１８】

また、前記取得したプレゼンス情報と前記取得したセキュリティポリシ情報とから新たに決定した送信ＩＰパケットのセキュリティポリシ情報を、前記他の通信装置に通知する構成とした。

【００１９】

さらに、前記取得したプレゼンス情報と前記取得したセキュリティポリシ情報とを表示し、前記新たに決定したセキュリティポリシ情報を入力するために周辺機器との外部インタフェースをさらに設けた。

【００２０】

【発明の実施の形態】

以下、本発明の実施形態について説明する。ここでは、通信網としてＩＰネットワークを用い、通信の安全性を確保するプロトコルとしてＩＰｓｅｃを用いた場合を例として説明する。

【００２１】

図１は本発明の通信装置１０の内部構成を説明する図である。本通信装置１０はＩＰネットワーク１を介して通信相手装置１１と通信を行う。なお、図１の通信装置１０は、以下に説明するセキュリティポリシの設定等に係る機能ブロックを中心に示したものであり、実際には、モバイル用ＰＣやＩＰ電話といった通信装置の種別によって異なる、他の図示しない機能ブロックを有している。また、通信相手装置１１も本通信装置１０と同一の機能構成を有するものとする。

【００２２】

本発明の通信装置１０は、ＩＰ機能ブロック１００、ＩＰｓｅｃ機能ブロック

１１０、ピアツーピア通信機能ブロック２００、セキュリティポリシデータベース３００、セキュリティポリシ処理部３０１、セキュリティポリシ入出力I/F３０２、プレゼンス情報データベース４００、プレゼンス情報処理部４０１、プレゼンス情報入出力Ｉ／Ｆ４０２、セキュリティポリシプレゼンス情報要求指示Ｉ／Ｆ４０３から構成される。

【００２３】

ＩＰ機能ブロック１００はデータパケットの送受信インタフェースであり、ＩＰパケットの終端および生成を行う。ＩＰｓｅｃ機能ブロック１１０はＩＰレイヤでのセキュリティを確保する機能ブロックであり、ＩＰパケットに対する認証および暗号化を行う。ピアツーピア通信機能ブロック２００はピアツーピア通信を実現する機能ブロックであり、通信装置間でのピアツーピア通信セッションの確立、確立したセッション上でのピアツーピア通信、および確立セッションの切断を行う。

【００２４】

セキュリティポリシデータベース３００は通信端末のセキュリティポリシを格納したデータベースであり、ＩＰｓｅｃ機能ブロックにて適用するセキュリティポリシの管理を行う。セキュリティポリシ処理部３０１はセキュリティポリシデータベースへのアクセスを行う機能ブロックであり、セキュリティポリシデータベースへのセキュリティポリシの登録や削除、ならびに参照を行う。セキュリティポリシ入出力インタフェース３０２はセキュリティポリシデータベースへのアクセスのためのユーザインタフェースであり、利用者に対し通信装置のセキュリティポリシデータベースへのアクセスを提供する。

【００２５】

セキュリティポリシプレゼンス情報要求指示インタフェース４０３はセキュリティポリシおよびプレゼンス情報の取得要求を行うためのユーザインタフェースであり、周辺機器２０等を介して、利用者に対し通信相手装置のセキュリティポリシやプレゼンス情報の取得要求を可能とする。プレゼンス情報データベース４００は通信端末のプレゼンス情報を格納したデータベースであり、通信装置のプレゼンス情報の管理を行う。

【００２６】

プレゼンス情報処理部４０１はプレゼンス情報データベースへのアクセスを行う機能ブロックであり、プレゼンス情報データベースへのプレゼンス情報の登録削除や参照を行う。プレゼンス情報入出力インタフェース４０２はプレゼンス情報データベースへのアクセスのためのユーザインタフェースであり、利用者に対し通信装置のプレゼンス情報データベースへのアクセス機能の提供を行う。

【００２７】

なお、上記のセキュリティポリシ入出力インタフェース３０２、セキュリティポリシプレゼンス情報要求指示インタフェース４０３およびプレゼンス情報入出力インタフェース４０２は、外部に別途用意されたディスプレイ装置、キーボード、マウス等の周辺機器２０に接続され、例えば、キーボードやマウス等を用いて各種情報の入力を行ったり、ディスプレイ装置を用いて出力情報の表示を行うことができる。

【００２８】

図２は通信装置１０が適用されるネットワーク構成を示す図である。ここでは、利用者９が通信装置１０を用い、社内ネットワーク２を介して通信相手装置Ａ１１－１とピアツーピア通信を行う場合と、社内ネットワーク２およびインターネット３を介して通信相手装置Ｂ１１－２とピアツーピア通信を行う場合とを示している。

【００２９】

なお、通信装置１０および通信相手装置Ａ１１－１のＩＰアドレスとしては、インターネットの標準化組織であるＩＥＴＦにて制定されたＲＦＣ１５９７に規定されたクラスＣのプライベートアドレスを想定し、それぞれ１９２．１６８．１．１および１９２．１６８．１．２とする。また、通信相手装置Ｂ１１－２のＩＰアドレスとしては、１３３．１３４．１０．１０として説明を行う。なお、以上のＩＰアドレスの値はあくまでも一例であり、他のアドレスであっても問題ない。

【００３０】

以下、図３～図９を用いて通信相手装置Ａ１１－１との通信方法を説明し、図

１０～図１３を用いて通信相手装置Ｂ１１－２との通信方法を説明する。

【００３１】

まず、社内ネットワーク２のみを介した通信装置１０と通信相手装置Ａ１１－１との通信方法を説明する。図３は、利用者９が通信装置１０を用いて通信相手装置Ａ１１－１とピアツーピア通信を開始する際のメッセージシーケンスである。

【００３２】

利用者９は、まず通信装置１０に対し、図１に示す周辺機器２０からセキュリティポリシプレゼンス情報要求指示Ｉ／Ｆ４０３を介して、通信相手装置Ａ１１－１のセキュリティポリシおよびプレゼンス情報の取得を指示する５０１。指示を受けた通信装置１０は、通信相手装置Ａ１１－１にプレゼンス情報およびセキュリティポリシを要求するメッセージをピアツーピア通信機能ブロック２００にて生成し、ＩＰ機能ブロック１００を介してＩＰパケットに載せて送信する５０２。

【００３３】

本パケットは通常のデータパケットと異なり、セキュリティポリシを交換するためのパケットであり、例えばＩｎｔｅｒｎｅｔ－Ｄｒａｆｔ（ｄｒａｆｔ－ＩＥＴＦ－ｉｍｐｐ－ｃｐｉｍ－ｐｉｄｆ－０７．ｔｘｔ）で規定されたフォーマットで生成されている。したがって、このＩＰパケットが受信側の通信相手装置Ａ１１－１のセキュリティポリシを満たしているかは不明であるが、この段階では受信側装置で廃棄されることなく受信される。

【００３４】

本要求メッセージを受信した通信相手装置Ａ１１－１は、プレゼンス情報およびセキュリティポリシを応答メッセージとしてＩＰパケットに載せて返信する５０３。通信装置１０は上記通信相手装置Ａ１１－１からの応答メッセージが載せられたＩＰパケットを受信すると、プレゼンス情報処理部４０１にて受信パケットの内容を解析することによって、相手通信装置Ａ１１－１のプレゼンス情報を抽出し、プレゼンス情報データベース４００に登録する５０４。そしてプレゼンス情報入出力Ｉ／Ｆ４０２から周辺機器２０を用いて、通信相手装置Ａ１１ａの

プレゼンス情報を利用者９に対して表示する５０５。

【００３５】

同様に、通信相手装置Ａ１１－１からの応答パケットをセキュリティポリシ処理部３０１にて解析することによって通信相手装置Ａ１１－１のセキュリティポリシデータを抽出し、セキュリティポリシ入出力Ｉ／Ｆ３０２から周辺機器２０を用い当該セキュリティポリシを利用者９に対して表示する５０６。

【００３６】

利用者９は、表示された通信相手装置Ａ１１－１における通信装置１０に対するセキュリティポリシの内容を検討し必要に応じて変更する。例えば、セキュリティレベルをより高く変更したり、あるいは低くする等を行う。

【００３７】

前記のように内容が見直されたセキュリティポリシは、セキュリティポリシ入出力Ｉ／Ｆ３０２から周辺機器２０を用い登録される５０７。登録の指示を受けた通信装置１０は、上記の通信相手装置Ａに対するセキュリティポリシを、セキュリティポリシ処理部３０１を介してセキュリティポリシデータベース３００に登録する５０８。

【００３８】

その後、利用者９はピアツーピア通信機能ブロック２００を介して通信相手装置Ａ１１－１とのピアツーピア通信の開始を指示し５０９、指示を受けた通信装置１０は、前記ピアツーピア通信機能ブロック２００を用いて通信相手装置Ａ１１－１とのピアツーピア通信を開始する５１０。

【００３９】

ピアツーピア通信機能ブロック２００には、周辺機器あるいは図示しない外部の装置や端末等から、通信相手装置に向けた通常の通信データが入力され、ＩＰｓｅｃ機能ブロックとの間で、相手装置との送受信データのＩＰアドレスやポート番号、上位プロトコルの種別を受渡しすることによって、セキュリティポリシデータベース３００に登録された前記セキュリティポリシに基づいたデータパケットが生成される。

【００４０】

図４は、図３のシーケンスにおける通信相手装置Ａ１１－１のセキュリティポリシおよびプレゼンス情報要求指示時５０１にて、セキュリティポリシプレゼンス情報要求指示Ｉ／Ｆ４０３が周辺機器２０のディスプレイ装置等に提供するＧＵＩ（グラフィカルユーザインタフェース）４１０の一例である。通信相手装置のアドレスをテキストボックス４１１に入力し、要求する情報のチェックボックス４１２、４１３をチェックし、ＯＫボタン４１４を押すことで要求を指示する。

【００４１】

図５に、図３のシーケンスにおける、通信相手装置Ａ１１－１からのプレゼンス情報およびセキュリティポリシ情報の応答５０３におけるプレゼンス情報およびセキュリティポリシの記述部分の一例を示す。ここでは、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）のＩＭＰＰ（Ｉｎｓｔａｎｔ Ｍｅｓｓａｇｉｎｇ ａｎｄ Ｐｒｅｓｅｎｃｅ Ｐｒｏｔｏｃｏｌ） ＷＧ（Ｗｏｒｋｉｎｇ Ｇｒｏｕｐ）にて作成中であるＰＩＤＦ（Ｐｒｅｓｅｎｃｅ Ｉｎｆｏｒｍａｔｉｏｎ Ｄａｔｅ Ｆｏｒｍａｔ）に準拠したフォーマットで作成されている。

【００４２】

図５において、５２０～５２６がセキュリティポリシに関する情報であり、５２７～５２８がプレゼンス情報である。なお、本メッセージは、例えばＩＥＴＦのＲＦＣ（Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ）３２６１に規定されたＳＩＰに代表されるピアツーピア通信プロトコルを用いて送受信が可能である。

【００４３】

図６は、図３のシーケンスにおいて通信相手装置Ａ１１－１のプレゼンス情報をプレゼンス情報データベース４００に登録した時５０４における、プレゼンス情報データベース４００の内容の一例である。各要素は、関連する通信装置のプレゼンス情報に対応し、端末の識別情報であるｅｎｔｉｔｙ６２０、端末のアドレス６２１、端末の現在の利用者名６２２、端末のある場所６２３、本プレゼンス情報が作成された日時６２４の各行から構成される。ここでは、６２５および６２７～６２９がそれぞれ図５のメッセージの５３０および５２７～５２９に対

応する。

【００４４】

図７は、図３のシーケンスにおいて通信相手装置Ａ１１－１に対するセキュリティポリシをセキュリティポリシデータベース３００に登録した時５０８のセキュリティポリシデータベース３００内容の一例である。各要素は通信相手装置１１に対するセキュリティポリシに対応し、送信元のアドレス７１０とそのポート番号７１１、送信先のアドレス７１２とそのポート番号７１３、トランスポート層のプロトコル７１４、送信か受信かを示す方向７１５、パケットに対してどのような処理を行うかを示すアクション７１６がある。

【００４５】

また、アクションにてｉｐｓｅｃを指定した場合についてはさらに、プロトコル７１７、モード７１８、エンドポイント７１９、レベル７２０の各行から構成される。ここでは、７２１～７２７がそれぞれ図５のメッセージの５１０～５１６に対応する。

【００４６】

図８に、前記通信相手装置Ａ１１－１との間のセキュリティポリシを表示した時５０６における、セキュリティポリシ入出力Ｉ／Ｆ３０２が周辺機器２０のディスプレイ装置等に提供するＧＵＩ８００の一例を示す。送信元および送信先のアドレスは、それぞれテキストボックス８１０および８１４に表示される。

【００４７】

特定のポートが指定されている場合は、テキストボックスのチェックボックス８１１および８１５が選択され、テキストボックス８１２および８１６に具体的なポート番号が表示される。特定のポートが指定されていない場合にはａｎｙのチェックボックス８１３および８１７が選択される。

【００４８】

トランスポート層のプロトコルは、対応するプロトコル名のラジオボタン８１８または８１９が選択される。プロトコルが指定されていない場合はａｎｙのラジオボタン８２０が選択される。パケットの送信方向は、受信パケットならばｉｎのラジオボタン８２１が選択され、送信方向ならばｏｕｔのラジオボタン８２

２が選択される。

【００４９】

パケットに対する処理については、パケット廃棄処理を行うならばｄｉｓｃａｒｄのラジオボタン８２３が選択され、何も処理を行わないのであればｎｏｎｅのラジオボタン８２４が選択され、ｉｐｓｅｃ処理を行うならばｉｐｓｅｃのラジオボタン８２５が選択される。

【００５０】

ｉｐｓｅｃのラジオボタンが選択されている場合には、さらに、適用するセキュリティプロトコルであるａｈ（認証）８２６、ｅｓｐ（暗号）８２７、ｉｐｃｏｍｐ（圧縮）８２８のそれぞれのチェックボックスが選択される。適用するモードがトランスポートモードかトンネルモードかはラジオボタン８２９または８３０を選択する。トンネルモードの場合は、トンネルのもう一方の端となる装置を示すテキストボックス８３１が表示され、セキュリティレベルとしてｄｅｆａｕｌｔ（デフォルト）８３２、ｕｓｅ（可能ならば）８３３、ｒｅｑｕｉｒｅ（必須）８３４のそれぞれのラジオボタンが表示される。

【００５１】

図８では、通信相手装置Ａ１１－１から受け取ったセキュリティポリシを元に、通信相手装置Ａ１１－１に対するセキュリティポリシとして、送信元アドレス１９２．１６８．１．１、ポートａｎｙ、送信先アドレス１９２．１６８．１．２、ポートａｎｙ、トランスポートｕｄｐ、方向ｏｕｔ、アクションｎｏｎｅがそれぞれ選択され、表示されている。通信相手装置Ａ１１－１は社内ＩＰネットワークに接続されているので、利用者はセキュリティポリシの変更は不要と判断し、このままのセキュリティポリシで登録ボタン８３５を押し、セキュリティポリシデータベースに登録を行う。

【００５２】

図９に前記通信相手装置Ａ１１－１のプレゼンス情報を表示した時５０５における、プレゼンス情報入出力Ｉ／Ｆ４０２が周辺機器のディスプレイ装置等に提供するＧＵＩ９００の一例を示す。

【００５３】

端末の識別情報であるｅｎｔｉｔｙ９１０、端末のアドレス９１１、端末の現在の利用者９１２、端末のある場所９１３、プレゼンス情報が作成された日時９１４がそれぞれ表示される。図９では、通信相手装置Ａから受け取ったプレゼンス情報として、ｅｎｔｉｔｙ　ｐｅｅｒＡ@ｅｘａｍｐｌｅ.ｃｏｍ９１７、アドレス１９２.１６８.１.２（９１８）、利用者Ｊｏｈｎ９１９、場所ｏｆｆｉｃｅ９２０、日時２００２－０９－２８　１０:４９:２９（９２１）がそれぞれ表示されている。したがって、通信装置の利用者は、通信装置Ａ１１－１が社内ＩＰネットワークに接続されていることを知ることができる。

【００５４】

なお、通信相手装置Ａ１１－１のプレゼンス情報はプレゼンス情報要求時にプレゼンス情報データベースに登録される。利用者はプレゼンス情報入出力Ｉ／Ｆを用いて、通信相手装置Ａ１１－１のプレゼンス情報のうち、利用者と場所の欄のみ利用者の好みに応じて親しみやすい値等に変更することが出来る。

【００５５】

次に、社内ＩＰネットワーク２とインターネット３とを介した通信装置１０と通信相手装置Ｂ１１－２との通信方法を説明する。図１０は、利用者９が通信装置１０を用いて通信相手装置Ｂ１１－２とピアツーピア通信を開始する際のメッセージシーケンスである。利用者９は、前述の通信装置Ａ１１－１と通信を行う場合と同様、通信装置１０に対し前記セキュリティポリシプレゼンス情報要求指示Ｉ／Ｆ４０３が周辺機器２０のディスプレイ装置等に提供するＧＵＩ等を用いて、通信相手装置Ｂ１１－２のセキュリティポリシおよびプレゼンス情報の要求を指示する６０１。

【００５６】

指示を受けた通信装置１０は、通信相手装置Ｂ１１－２にプレゼンス情報およびセキュリティポリシを要求するメッセージを送信する６０２。通信相手装置Ｂ１１－２はプレゼンス情報およびセキュリティポリシを応答するメッセージを返信する６０３。

【００５７】

応答メッセージを受信した通信装置１０は、通信相手装置Ｂ１１－２のプレゼ

ンス情報を前記プレゼンス情報データベース４００に登録し６０４、前記プレゼンス情報入出力Ｉ／Ｆ４０２を用いて周辺機器２０のディスプレイ装置等に通信相手装置Ｂ１１－２のプレゼンス情報を表示する６０５。また、前記セキュリティポリシ入出力Ｉ／Ｆ３０２を用いて周辺機器２０のディスプレイ装置等に通信相手装置Ｂ１１－２との間のセキュリティポリシを表示する６０６。以上は前述の図３に示した社内ＩＰネットワーク２を介した通信相手装置Ａ１１－１とのメッセージシーケンスと同一である。

【００５８】

ここで、利用者９は表示された通信相手装置Ｂ１１－２のプレゼンス情報を解析することによって、通信相手装置Ｂ１１－２の現状の接続先が社外のネットワークであることが分かる。

【００５９】

図１１は、図１０のシーケンスにおいて前記通信相手装置Ｂのプレゼンス情報を表示した時６０５の、外部のディスプレイ装置へのＧＵＩ１１０の一例である。場所９３０がｓｔａｔｉｏｎとなっており、通信相手装置Ｂ１１－２が社外ネットワークに接続されていることが判る。そこで、別途表示された通信相手装置Ｂ１１－２との間のセキュリティポリシの内容を解析し、セキュリティレベルが現状に相応なものか否かを判断する。

【００６０】

図１２は、このときのセキュリティポリシの外部ディスプレイ装置へのＧＵＩ１２００の一例である。通信パケットに対する処理がｎｏｎｅ８５０となっているため、通信パケットに対するセキュリティ処理を行わないポリシであることを示している。なお、これは図８に示した社内ＩＰネットワークのみを介した通信を前提としたセキュリティポリシと同等である。

【００６１】

このような場合、通信の安全性を確保するためのセキュリティポリシとしては十分でないと判断し、図１０のシーケンス６０８に示すように、利用者９は通信相手装置Ｂ１１－２に対するセキュリティポリシをレベルのより高いものに変更する。そして利用者９は通信装置１０に対して、その変更後のセキュリティポリ

シの登録を指示し６０９、指示を受けた通信装置１０は、前記セキュリティポリシデータベース３００に登録する６１０。

【００６２】

図１３はこの変更時における、セキュリティポリシの外部ディスプレイ装置へのＧＵＩ１３００の一例である。すなわち、先の図１１が変更前、本図１３が変更後に相当するものである。通信相手装置Ｂ１１－２のプレゼンス情報から通信相手装置Ｂ１１－２が社外ネットワークに接続していることが明らかとなったため、通信相手装置Ｂ１１－２への送信パケットに対して、セキュリティ処理（ｉｐｓｅｃ８６０）を行うこととし、認証（ａｈ８６１）、暗号化（ｅｓｐ８６２）を必須（ｒｅｑｕｉｒｅ８６５）としていることを示している。

【００６３】

その後、利用者９は通信相手装置Ｂ１１－２とのピアツーピア通信の開始を指示し６１１、指示を受けた通信装置１０は、前記ピアツーピア通信機能ブロック２００を用いて通信相手装置Ｂ１１－２とのピアツーピア通信を開始する６１２。

【００６４】

ここで、通信相手装置Ｂ１１－２が保持している通信装置１０からの受信パケットに関するセキュリティポリシ（ＳＰ１）と、通信装置１０が保持している通信相手装置Ｂ１１－２への送信パケットに関するセキュリティポリシ（ＳＰ２）とを比較すると、ＳＰ１に比べてＳＰ２の方がそのセキュリティレベルが高いものとなっている。

【００６５】

しかしながら、受信側（通信相手装置Ｂ１１－２）で設定している以上のセキュリティレベルで送信されたパケットについては、受信側でそのまま受信してもセキュリティ上の問題はない。したがって、通信に先立って通信装置１０から通信相手装置Ｂ１１－２に対してセキュリティポリシの変更やそのネゴシエーションを実施することは必ずしも必要でない。

【００６６】

これに対して、前述のセキュリティポリシの変更時６０８において、変更後の

セキュリティポリシのセキュリティレベルが通信相手装置Ｂ１１－２にて保持するものと比して低くなるよう変更した場合、通信相手装置Ｂ１１－２では自ら設定しているより低いセキュリティレベルの受信パケットは廃棄等の処理が行われるため、通信装置１０は通信に先立って通信相手装置Ｂ１１－２とセキュリティポリシの変更に関してネゴシエーションが必要となる。

【００６７】

なお、以上の実施例では、セキュリティ通信プロトコルとしてＩＰｓｅｃを前提として説明を行ったが、ＩＰｓｅｃ機能ブロックを置き換えることによって、他のセキュリティ通信プロトコルにも適用可能である。また、セキュリティポリシデータベースやプレゼンス情報データベースは必ずしもデータベースである必要はなく、メモリ上のテーブルでも実現可能である。

【００６８】

【発明の効果】

以上のように本発明によれば、ピアツーピア通信において通信端末や使用者の状況に応じた適切なセキュリティポリシを用いた通信が可能となる。また、適切なセキュリティポリシを選択可能とすることにより、過剰なセキュリティレベルでのピアツーピア通信を防ぎ、通信端末でのＣＰＵリソースや通信ネットワークの帯域の節約が可能となる。

【図面の簡単な説明】

【図１】

本発明の通信装置の内部ブロック図を説明する図である。

【図２】

本発明の通信装置の適用されるネットワーク構成を説明する図である。

【図３】

本発明のメッセージシーケンスを説明する図である。

【図４】

本発明のＧＵＩ表示の一例を説明する図である。

【図５】

本発明のプレゼンス情報およびセキュリティポリシの記述部分を説明する図で

ある。

【図６】

本発明のプレゼンス情報データベースの構成を説明する図である。

【図７】

本発明のセキュリティポリシデータベースの構成を説明する図である。

【図８】

本発明のＧＵＩ表示の一例を説明する図である。

【図９】

本発明のＧＵＩ表示の一例を説明する図である。

【図１０】

本発明のメッセージシーケンスを説明する図である。

【図１１】

本発明のＧＵＩ表示の一例を説明する図である。

【図１２】

本発明のＧＵＩ表示の一例を説明する図である。

【図１３】

本発明のＧＵＩ表示の一例を説明する図である。

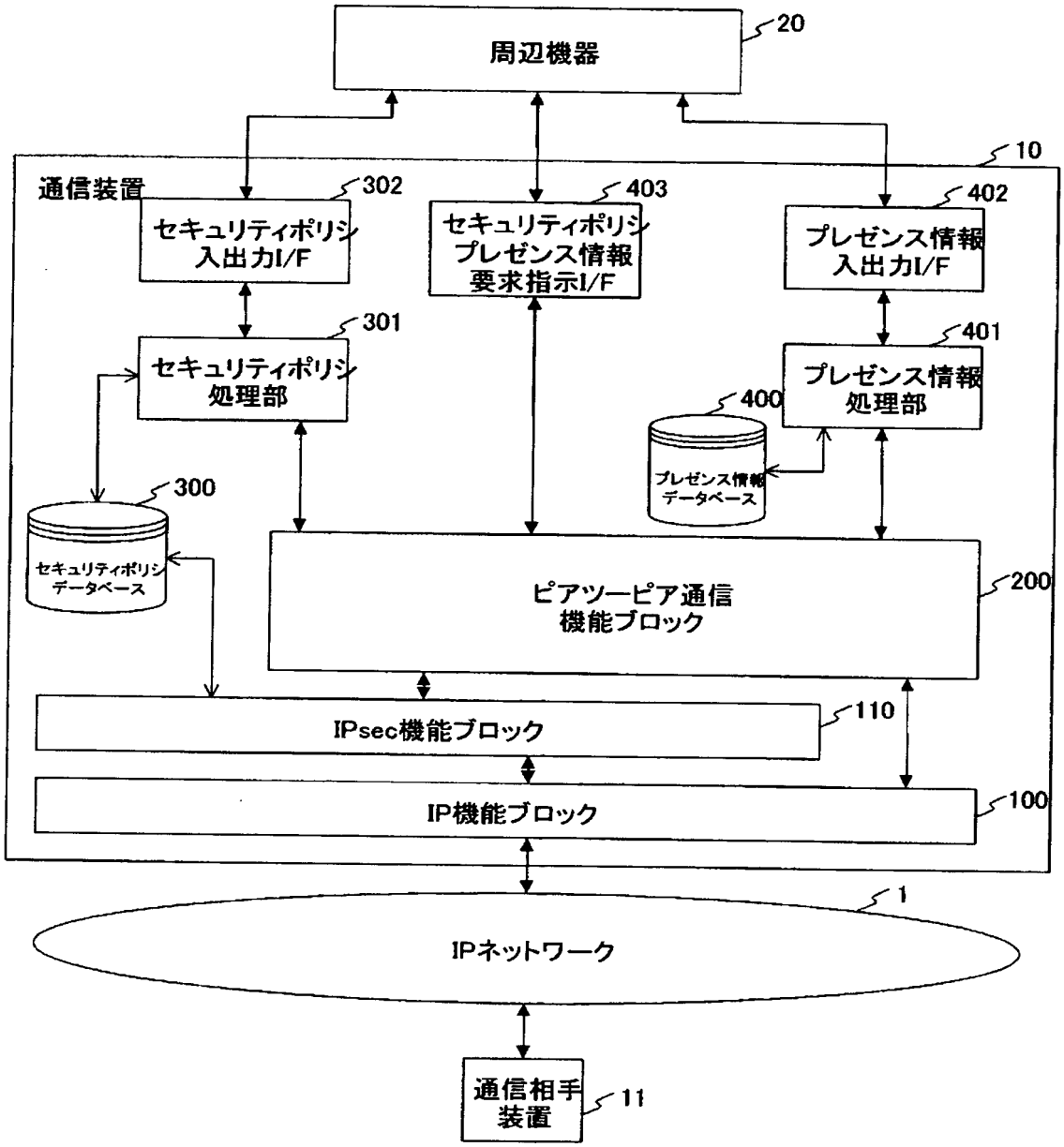
【符号の説明】

１･･･ＩＰネットワーク、２･･･社内ネットワーク、３･･･インターネット、９･･･利用者、１０･･･通信装置、１１･･･通信相手装置、１００･･･ＩＰ機能ブロック、１１０･･･ＩＰｓｅｃ機能ブロック、２００･･･ピアツーピア通信機能ブロック、３００･･･セキュリティポリシデータベース、３０１･･･セキュリティポリシ処理部、３０２･･･セキュリティポリシ入出力Ｉ／Ｆ、４００･･･プレゼンス情報データベース、４０１･･･プレゼンス情報処理部、４０２･･･プレゼンス情報入出力Ｉ／Ｆ、４０３･･･セキュリティポリシプレゼンス情報要求指示Ｉ／Ｆ

【書類名】　図面

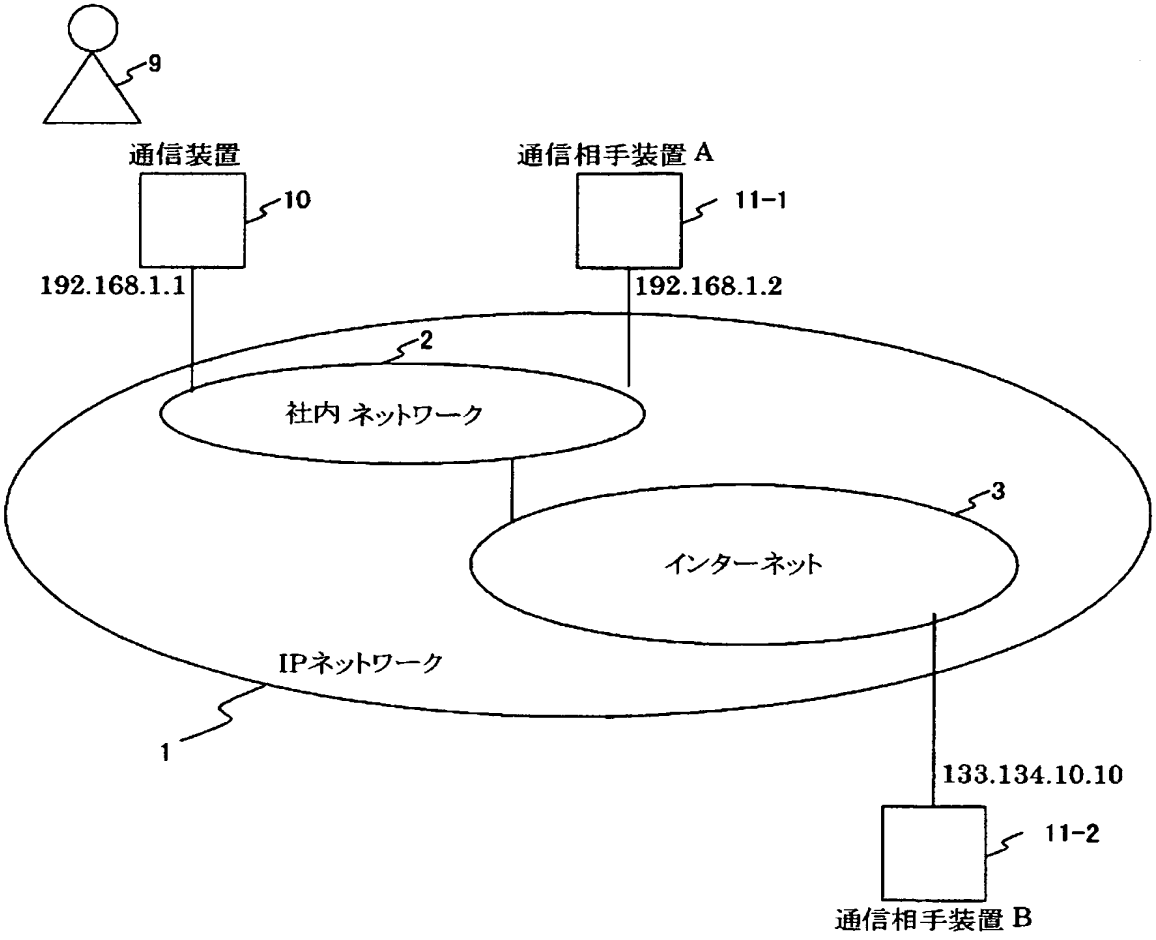
【図１】

【図1】


周辺機器
20
10
通信装置
302
セキュリティポリシ
入出力I/F
403
セキュリティポリシ
プレゼンス情報
要求指示I/F
402
プレゼンス情報
入出力I/F
301
セキュリティポリシ
処理部
401
プレゼンス情報
処理部
400
プレゼンス情報
データベース
300
セキュリティポリシ
データベース
ピアツーピア通信
機能ブロック
200
IPsec機能ブロック
110
IP機能ブロック
100
1
IPネットワーク
通信相手
装置
11

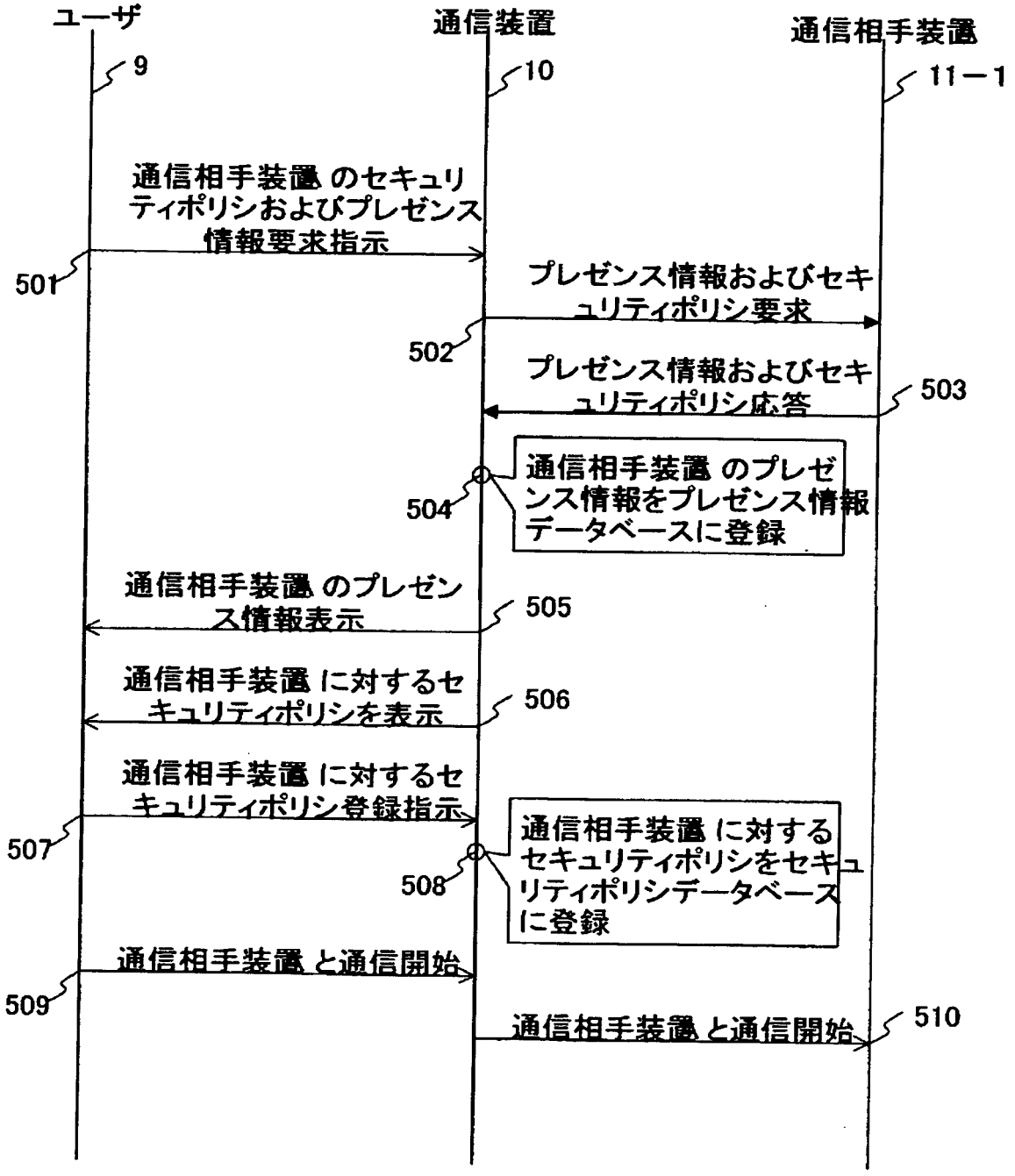
【図２】

【図2】


9
通信装置
10
192.168.1.1
通信相手装置 A
11-1
192.168.1.2
2
社内 ネットワーク
3
インターネット
IPネットワーク
1
133.134.10.10
11-2
通信相手装置 B

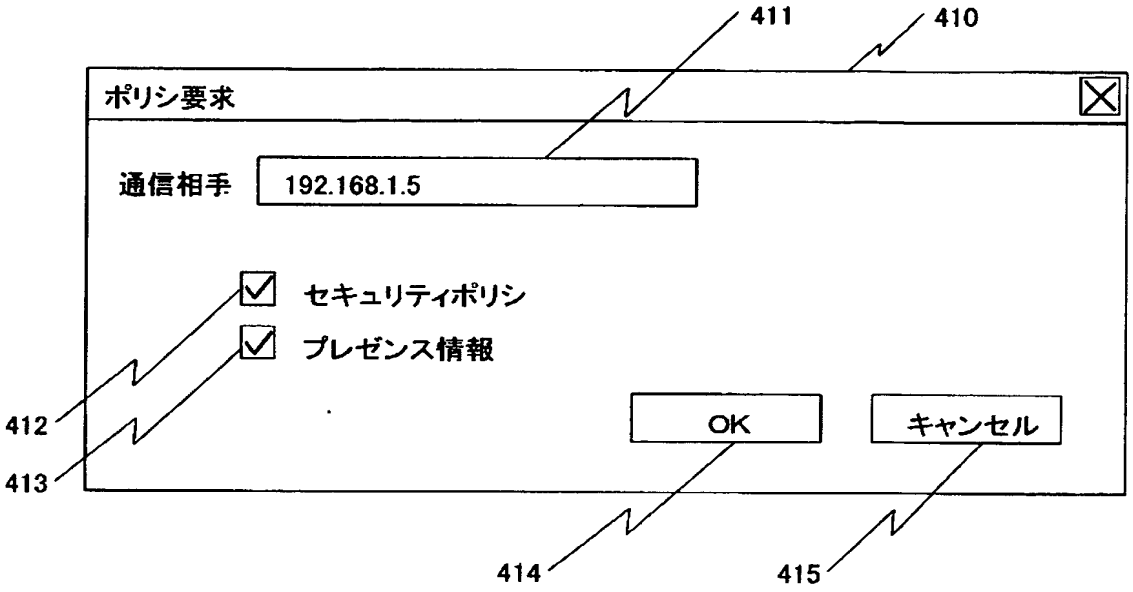
【図３】

【図3】


ユーザ
通信装置
通信相手装置
9
10
11－1
通信相手装置のセキュリティポリシおよびプレゼンス情報要求指示
501
プレゼンス情報およびセキュリティポリシ要求
502
プレゼンス情報およびセキュリティポリシ応答
503
通信相手装置のプレゼンス情報をプレゼンス情報データベースに登録
504
通信相手装置のプレゼンス情報表示
505
通信相手装置に対するセキュリティポリシを表示
506
通信相手装置に対するセキュリティポリシ登録指示
507
通信相手装置に対するセキュリティポリシをセキュリティポリシデータベースに登録
508
通信相手装置と通信開始
509
通信相手装置と通信開始
510

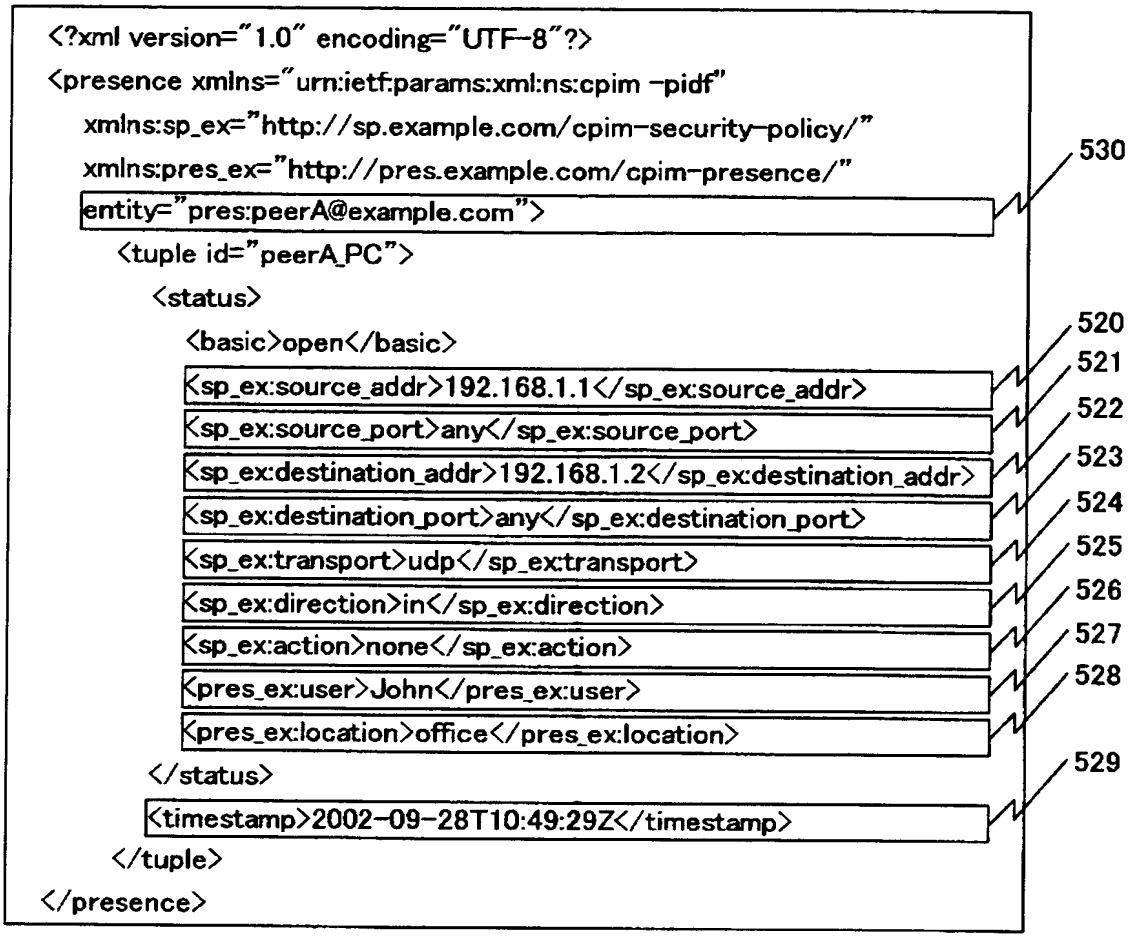
【図４】

【図4】


411
410
ポリシ要求
通信相手
192.168.1.5
セキュリティポリシ
プレゼンス情報
412
413
OK
キャンセル
414
415

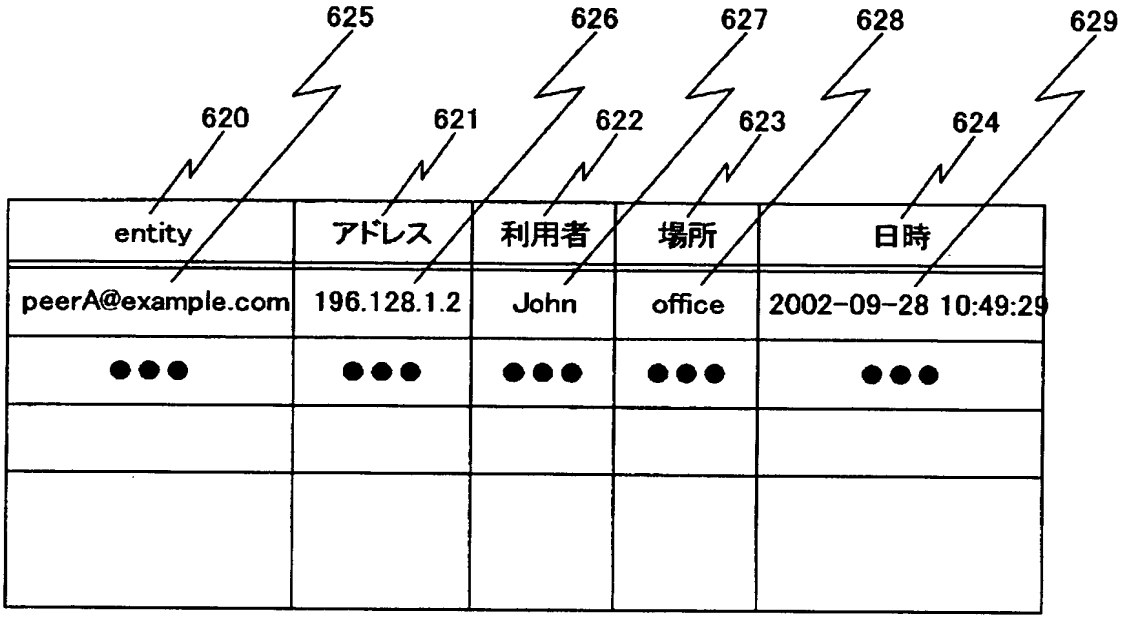
【図５】

【図5】


<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:cpim -pidf"
xmlns:sp_ex="http://sp.example.com/cpim-security-policy/"
xmlns:pres_ex="http://pres.example.com/cpim-presence/"
entity="pres:peerA@example.com">
<tuple id="peerA_PC">
<status>
<basic>open</basic>
<sp_ex:source_addr>192.168.1.1</sp_ex:source_addr>
<sp_ex:source_port>any</sp_ex:source_port>
<sp_ex:destination_addr>192.168.1.2</sp_ex:destination_addr>
<sp_ex:destination_port>any</sp_ex:destination_port>
<sp_ex:transport>udp</sp_ex:transport>
<sp_ex:direction>in</sp_ex:direction>
<sp_ex:action>none</sp_ex:action>
<pres_ex:user>John</pres_ex:user>
<pres_ex:location>office</pres_ex:location>
</status>
<timestamp>2002-09-28T10:49:29Z</timestamp>
</tuple>
</presence>
530
520
521
522
523
524
525
526
527
528
529

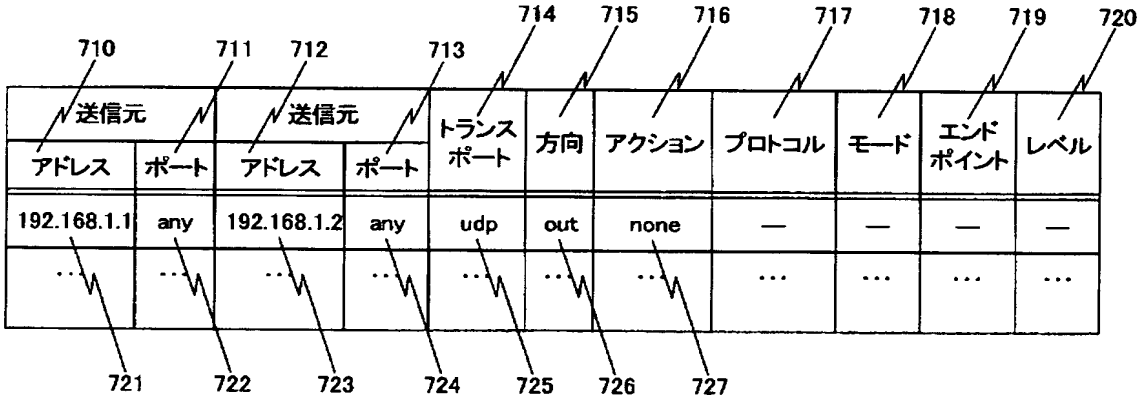
【図６】

【図6】


625
626
627
628
629
620
621
622
623
624
entity
アドレス
利用者
場所
日時
peerA@example.com
196.128.1.2
John
office
2002-09-28 10:49:29

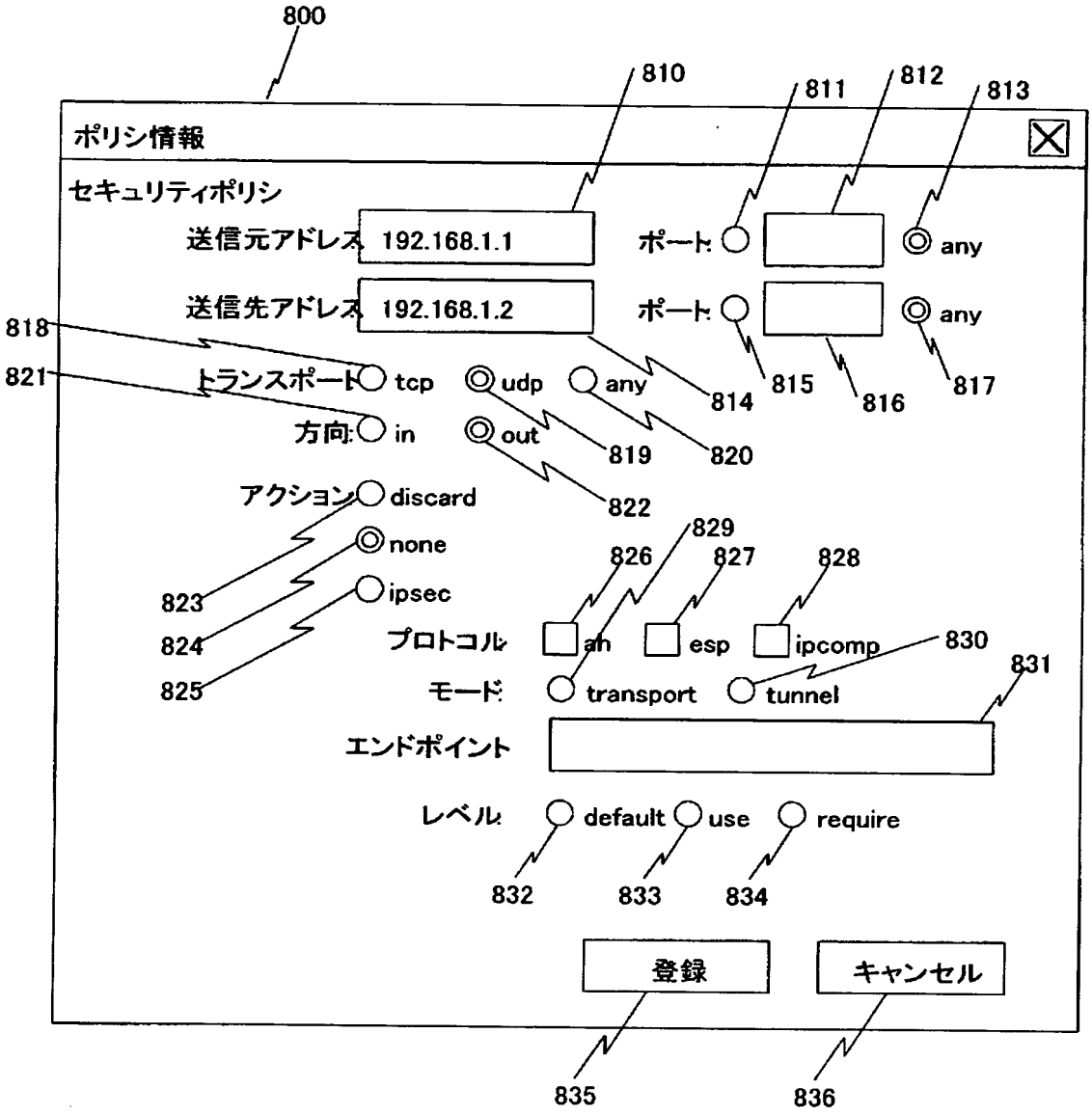
【図７】

【図7】


710
711
712
713
714
715
716
717
718
719
720
送信元
送信元
アドレス
ポート
アドレス
ポート
トランスポート
方向
アクション
プロトコル
モード
エンドポイント
レベル
192.168.1.1
any
192.168.1.2
any
udp
out
none
—
—
—
—
721
722
723
724
725
726
727

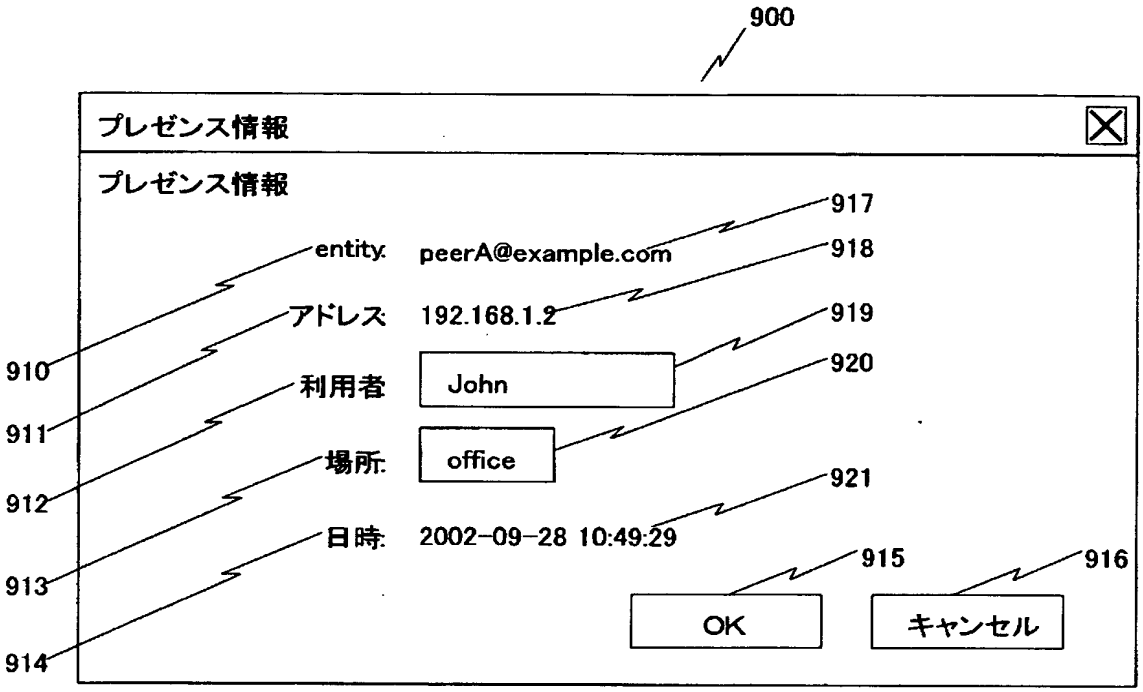
【図８】

【図8】

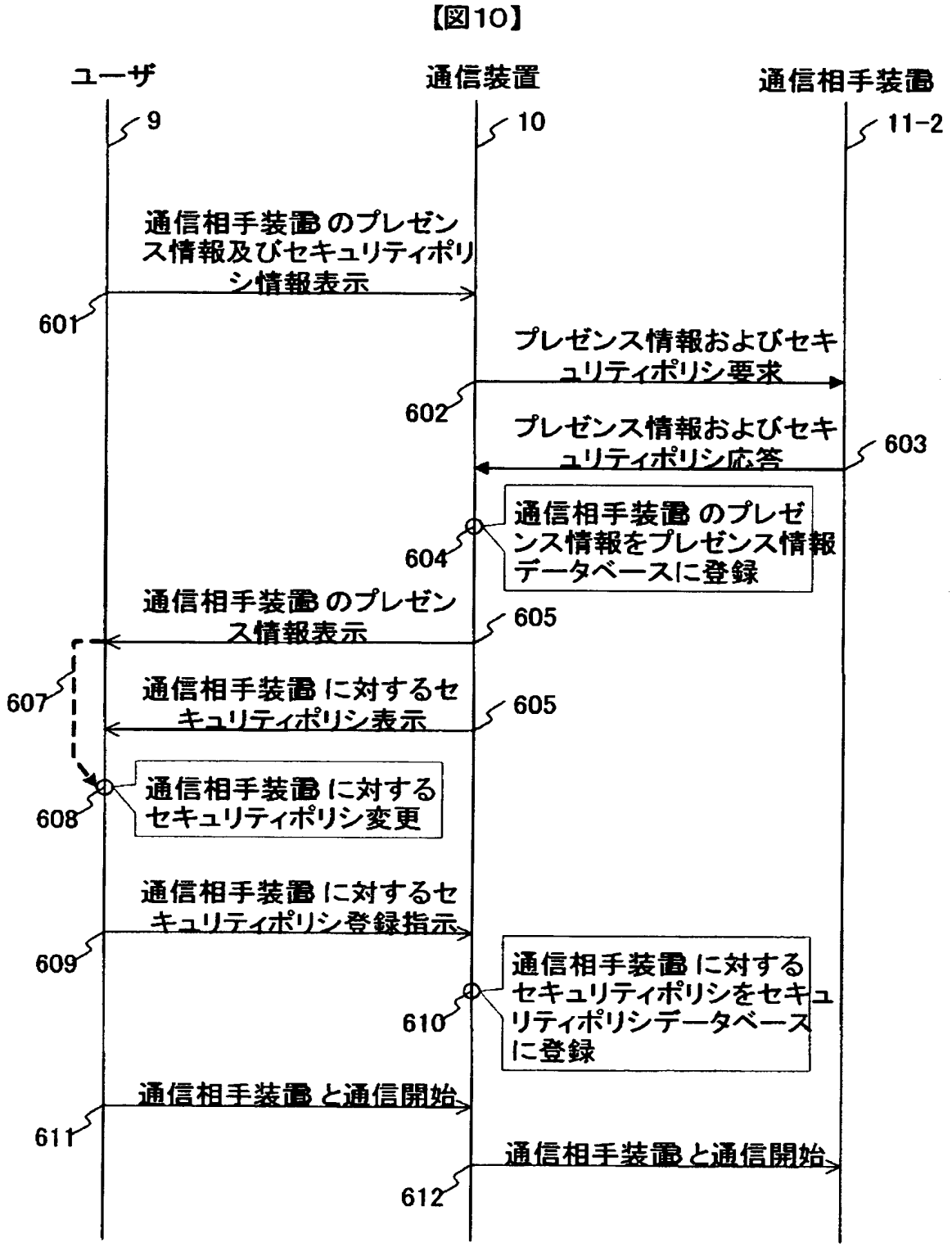

800
810
811
812
813
ポリシ情報
セキュリティポリシ
送信元アドレス
192.168.1.1
ポート:
any
送信先アドレス
192.168.1.2
ポート:
any
818
821
トランスポート
tcp
udp
any
814
815
816
817
方向:
in
out
819
820
アクション
discard
822
none
829
826
827
828
823
ipsec
824
プロトコル
ah
esp
ipcomp
830
825
モード
transport
tunnel
831
エンドポイント
レベル
default
use
require
832
833
834
登録
キャンセル
835
836

【図９】

【図9】

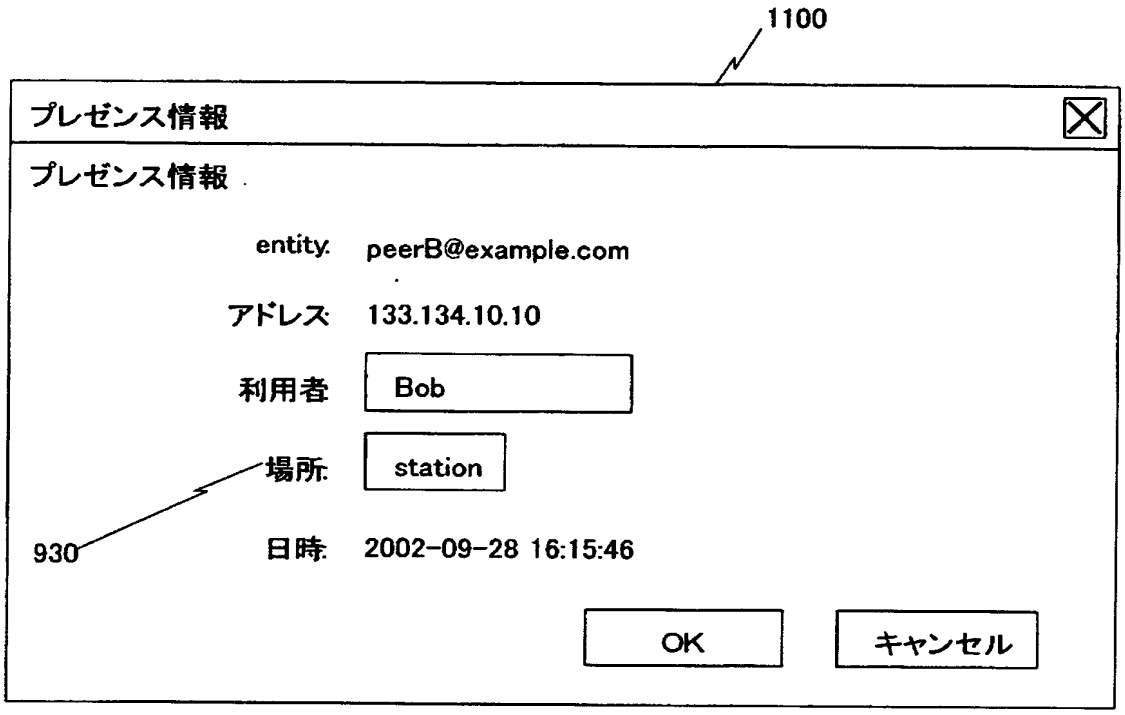

900
プレゼンス情報
プレゼンス情報
entity:
peerA@example.com
アドレス:
192.168.1.2
利用者:
John
場所:
office
日時:
2002-09-28 10:49:29
OK
キャンセル
910
911
912
913
914
915
916
917
918
919
920
921

【図１０】


【図10】
ユーザ
通信装置
通信相手装置
9
10
11-2
通信相手装置のプレゼンス情報及びセキュリティポリシ情報表示
601
プレゼンス情報およびセキュリティポリシ要求
602
プレゼンス情報およびセキュリティポリシ応答
603
通信相手装置のプレゼンス情報をプレゼンス情報データベースに登録
604
通信相手装置のプレゼンス情報表示
605
607
通信相手装置に対するセキュリティポリシ表示
605
通信相手装置に対するセキュリティポリシ変更
608
通信相手装置に対するセキュリティポリシ登録指示
609
通信相手装置に対するセキュリティポリシをセキュリティポリシデータベースに登録
610
通信相手装置と通信開始
611
通信相手装置と通信開始
612

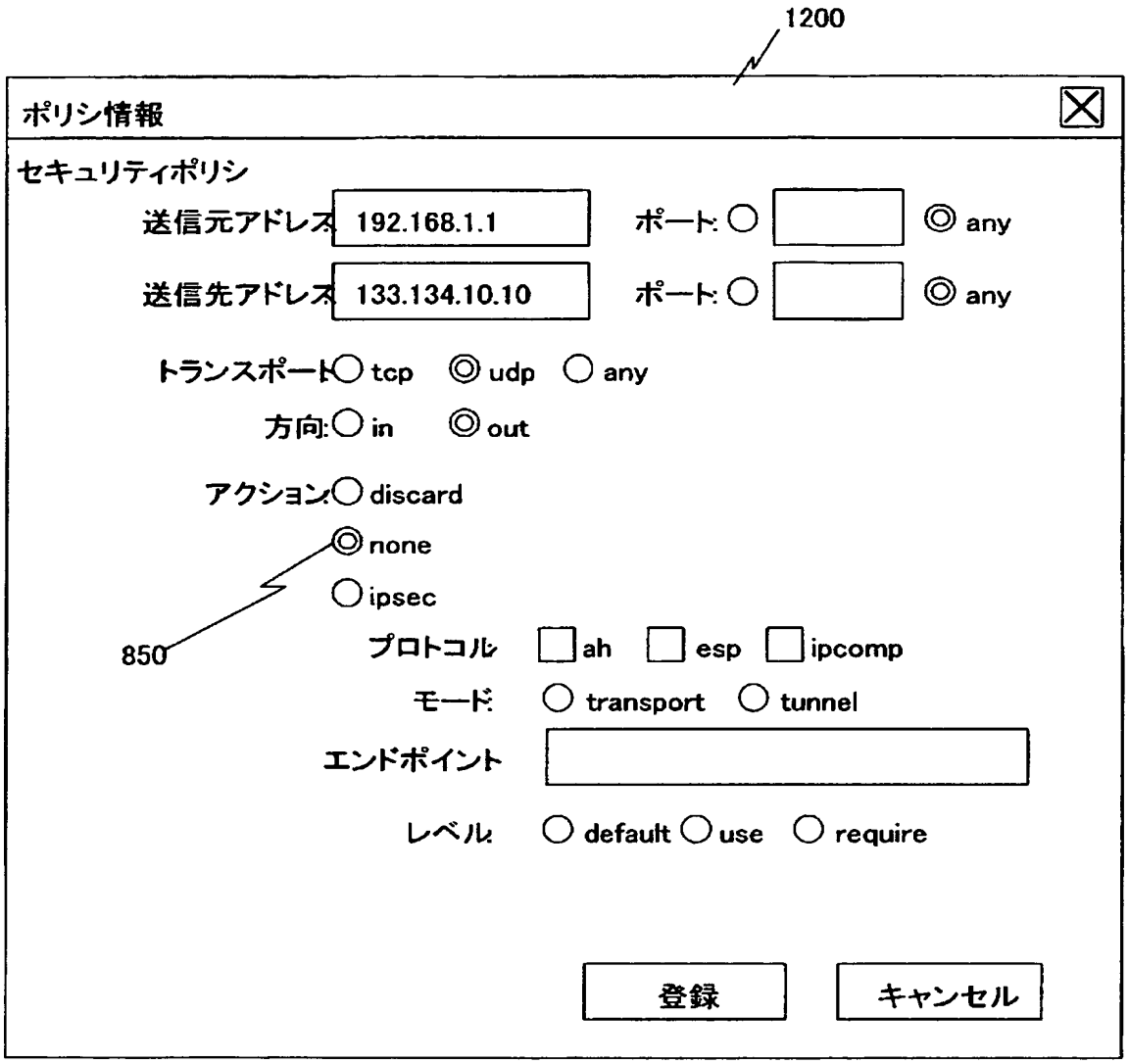
【図１１】

【図11】


1100
プレゼンス情報
プレゼンス情報
entity:
peerB@example.com
アドレス:
133.134.10.10
利用者:
Bob
場所:
station
930
日時:
2002-09-28 16:15:46
OK
キャンセル

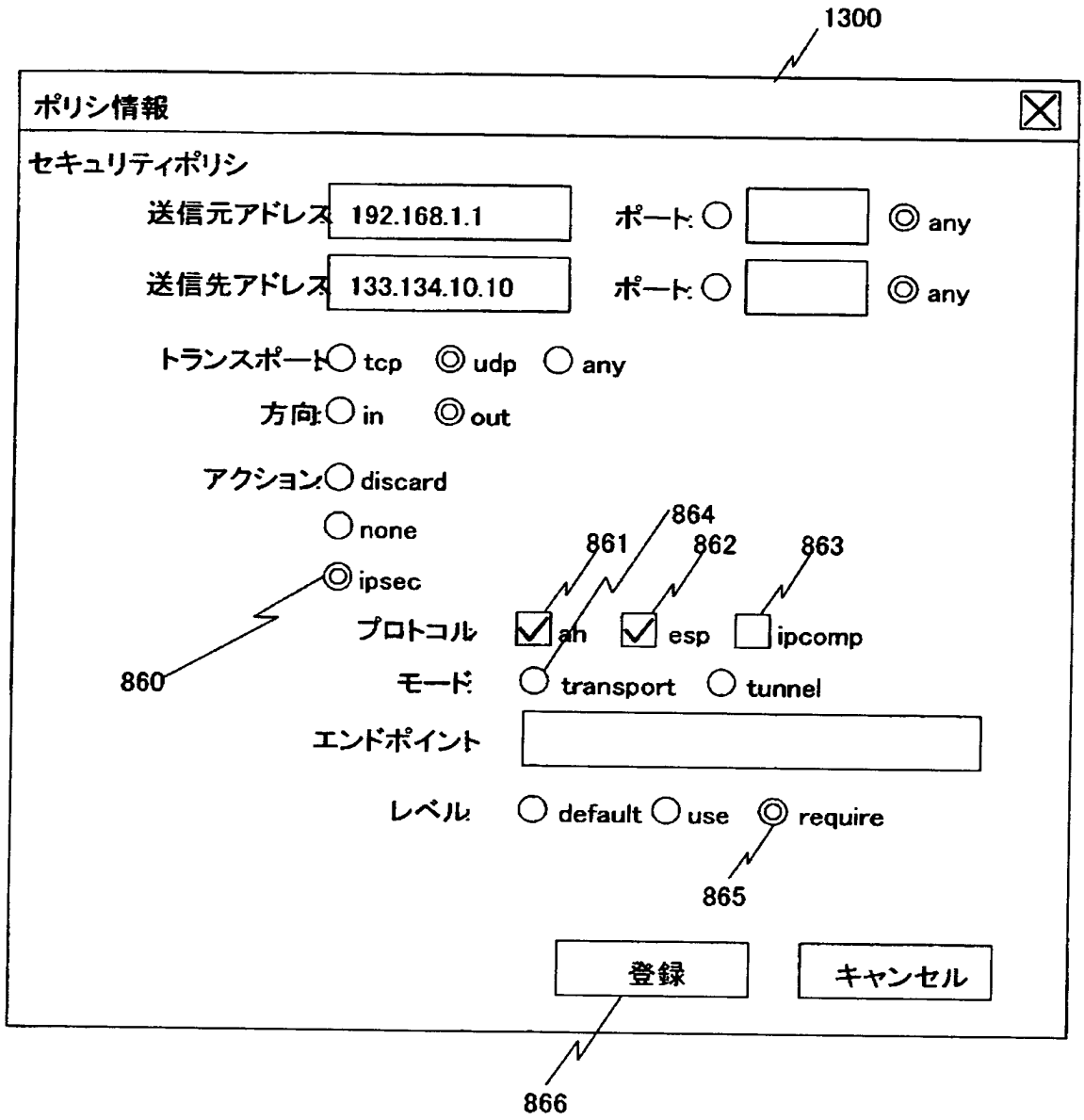
【図１２】

【図12】


1200
ポリシ情報
セキュリティポリシ
送信元アドレス
192.168.1.1
ポート:
any
送信先アドレス
133.134.10.10
ポート:
any
トランスポート
tcp
udp
any
方向:
in
out
アクション:
discard
none
ipsec
850
プロトコル
ah
esp
ipcomp
モード:
transport
tunnel
エンドポイント
レベル:
default
use
require
登録
キャンセル

【図１３】

【図13】


1300
ポリシ情報
セキュリティポリシ
送信元アドレス
192.168.1.1
ポート
any
送信先アドレス
133.134.10.10
ポート
any
トランスポート
tcp
udp
any
方向
in
out
アクション
discard
none
ipsec
860
861
862
863
864
プロトコル
ah
esp
ipcomp
モード
transport
tunnel
エンドポイント
レベル
default
use
require
865
登録
キャンセル
866

【書類名】　要約書

【要約】

【課題】

安全性が確保されたピアツーピア通信を実現するために、通信パケットに対する暗号および認証規則を示すセキュリティポリシおよび通信装置の通信状況を示すプレゼンス情報を通信装置間で互いに交換し、通信状況に応じた適切なセキュリティポリシを用いたセキュアなピアツーピア通信を可能とする通信装置を提供する。

【解決手段】

ＩＰネットワークに接続された他の通信装置が属するネットワークおよび前記他の通信装置の利用者に関するプレゼンス情報を取得する手段と、前記他の通信装置の通信パケットの送受信における一連の暗号および認証規則を示すセキュリティポリシ情報を取得する手段とを備え、前記プレゼンス情報と前記セキュリティポリシ情報とから、前記他の通信装置に送信するＩＰパケットのセキュリティポリシを決定し、前記決定したセキュリティポリシを用いて前記他の通信装置にＩＰパケットを送信する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０６４３２８
受付番号	５０３００３８９５３７
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　３月１２日

＜認定情報・付加情報＞

【提出日】　平成15年 3月11日

次頁無

特願２００３－０６４３２８

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所